Flowspec – TA505's bulletproof hoster of choice

intel471.com/blog/bulletproof-hoster-of-choice

By the Intel 471 Intelligence Analysis team.

Here at Intel 471 we spend a fair amount of time tracking malicious infrastructure providers. In the world of cybercrime the malicious infrastructure provider, or Bulletproof Hoster (BPH) as they are called in the underground marketplace, is a core enabling service that often gets little attention from threat intelligence analysts. It's difficult to quantify their impact as it's often spread over the activities of many different clients that are conducting activities that range from low-level phishing to more sophisticated intrusions. Sure, IP addresses and domains associated with badness get pushed over to the NOC/SOC, SIEM or endpoints to protect the enterprise, but few are digging beyond the initial incident and indicators then working up the chain to prefixes, Autonomous System Numbers (ASN) or even the companies behind them.

As you divert your attention to the malicious infrastructure provider and move up this chain, you're dealing with aspects of the bad guy's business model that are more costly to put in place and thus change less frequently. You're also allowing for opportunities to identify, track and proactively block clusters of infrastructure that, while not yet used for malicious activity, have been set aside for such badness. In this blog we'll start with some infrastructure suspected to be in use by TA505 and make the case for blocking the entire associated prefix as well as using BGP announcements to monitor for future indications of infrastructure being put in place.

Through the course of our research we've identified a couple of IPs addresses suspected to have been used in secondary activity by TA505, so if you're seeing these then it means you've potentially got some big problems.

```
176.121.14.175

176.121.14.238
```

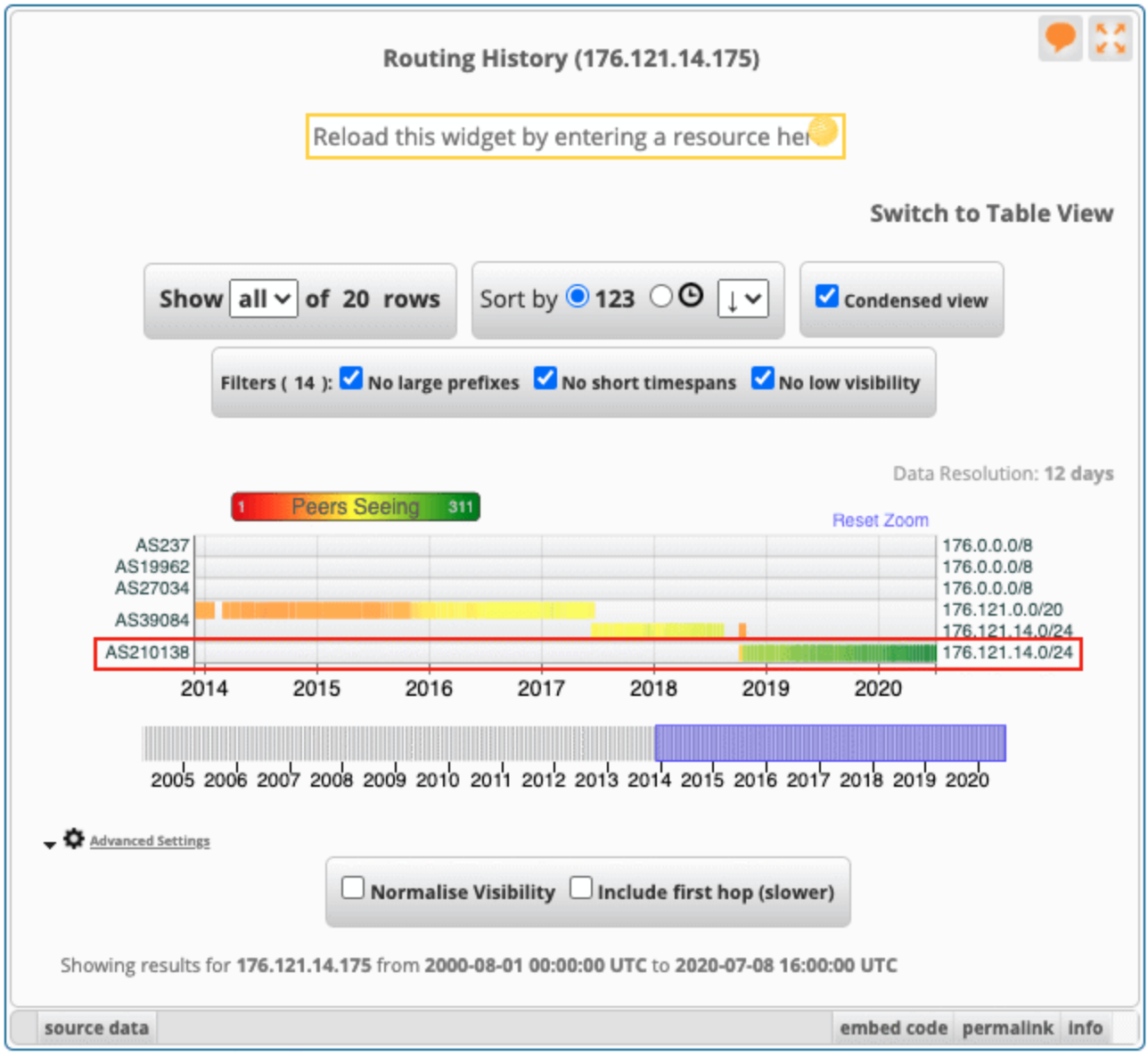
These are a bit more significant to TA505 operations than Get2 Loader malware infrastructure, which are used early on as part of the initial infection. Get2 Loader is widely thought to be the loader operated by TA505 early on in their intrusions. This infrastructure will typically see more frequent turnover given its position in the chain, but the same exercise can be done with those domains & IPs as well…and it's worth doing.

When looking at an IP address there are few red flags that should get your attention. It's certainly not a perfect science, but they do offer indications you may be dealing with BPH infrastructure set aside to support malicious activity.

1. Things to look out for include:
2. The associated company is registered to an offshore location such as Belize, Seychelles, Panama or others;
3. The company was registered in the last 1-3 years;
4. The associated ASNs were created in the last 1-3 years;
5. There are only a small number (1 – 6) prefixes associated with the ASN;
6. The prefixes associated with the ASN are smaller (/22 to /24);
7. The ASN has a small number (1 – 2) of peers (as in BGP peering);
8. Little or no benign content is hosted within the infrastructure;
9. The organization maintains a presence in the underground marketplace…obvious giveaway!

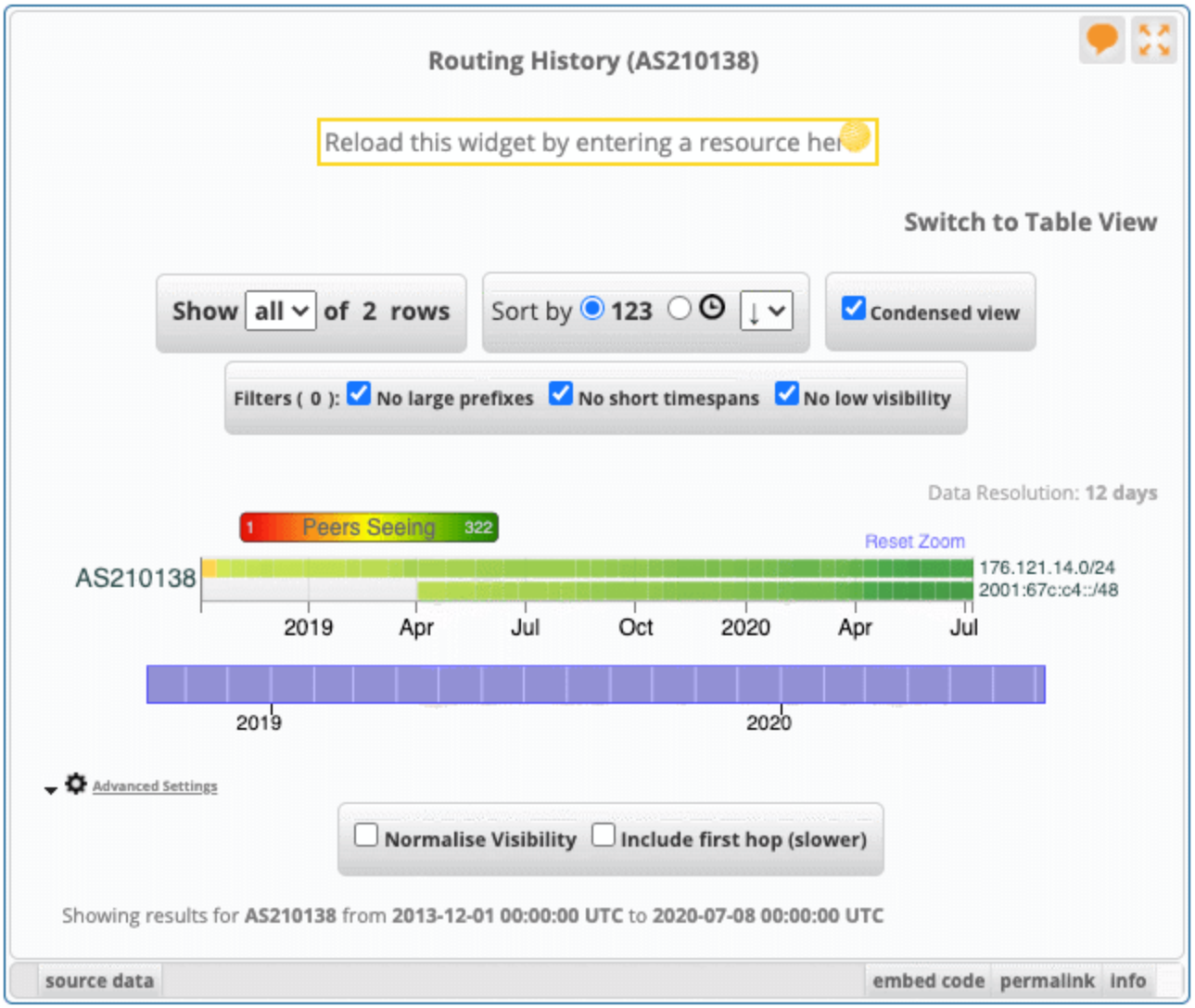
To give a quick and simple example we'll start with the two IPs mentioned above as being associated with TA505 activity. The first thing we want to understand is the smallest prefix announcement and routing history associated with the IP address. That's pretty easy using RIPE's free tool RIPEStat. The key takeaways from the screens below are that both IPs have been part of 176.121.14.0/24 since mid-2018 and it is currently announced by AS210138. Also, this prefix provides a fairly small number of IP addresses — 256 to be exact.

https://stat.ripe.net/widget/routing-history#w.resource=176.121.14.175



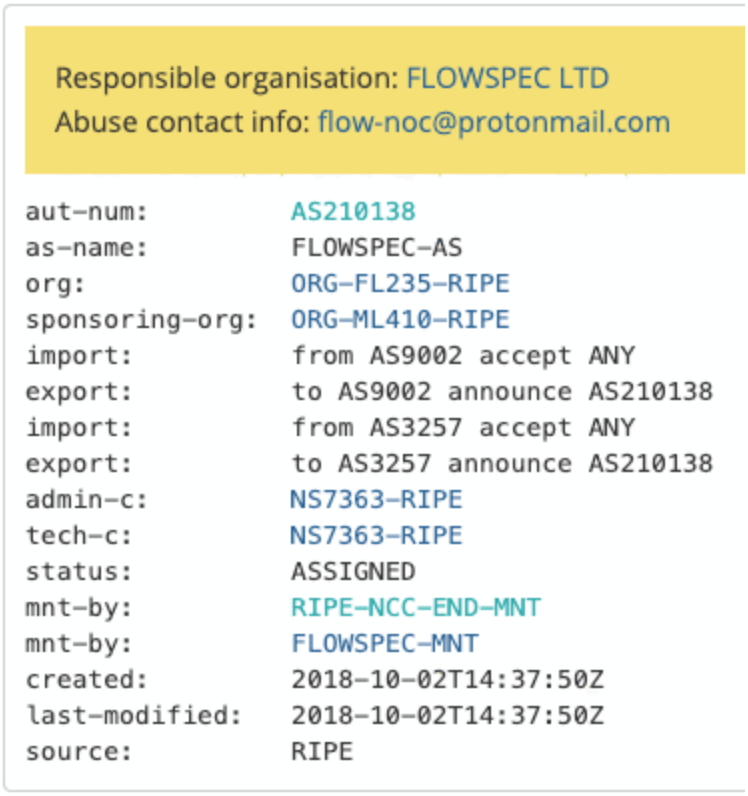
We can also use RIPEStat to understand the routing history for AS210138. This will provide you information related to what other prefixes have been and are being announced under a particular Autonomous System (AS). What we can see is that AS210138 has only announced the subject /24 IPv4 prefix since October 2019 and the IPv6 /48 since in April 2020. If you were confident an ASN was controlled by a malicious infrastructure provider you could make the case for blocking any prefixes associated with it currently and in the future.

https://stat.ripe.net/widget/routing-history#w.resource=AS210138



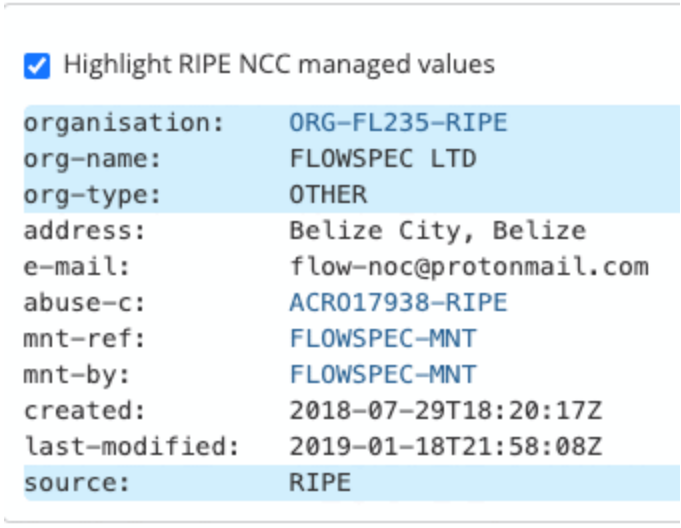
We can look further into the ASN, the parent organization, and more using the RIPE database and other tools, but that's beyond the scope of this blog. We'll stick to three RIPE objects (person, organization and ASN) that provide some pretty decent insight into the AS and those that control it.

https://apps.db.ripe.net/db-web-ui/lookup?source=ripe&key=AS210138&type=aut-num



https://apps.db.ripe.net/db-web-ui/lookup?source=ripe&key=ORG-FL235-RIPE&type=organisation

https://apps.db.ripe.net/db-web-ui/lookup?source=RIPE&type=person&key=NS7363-RIPE



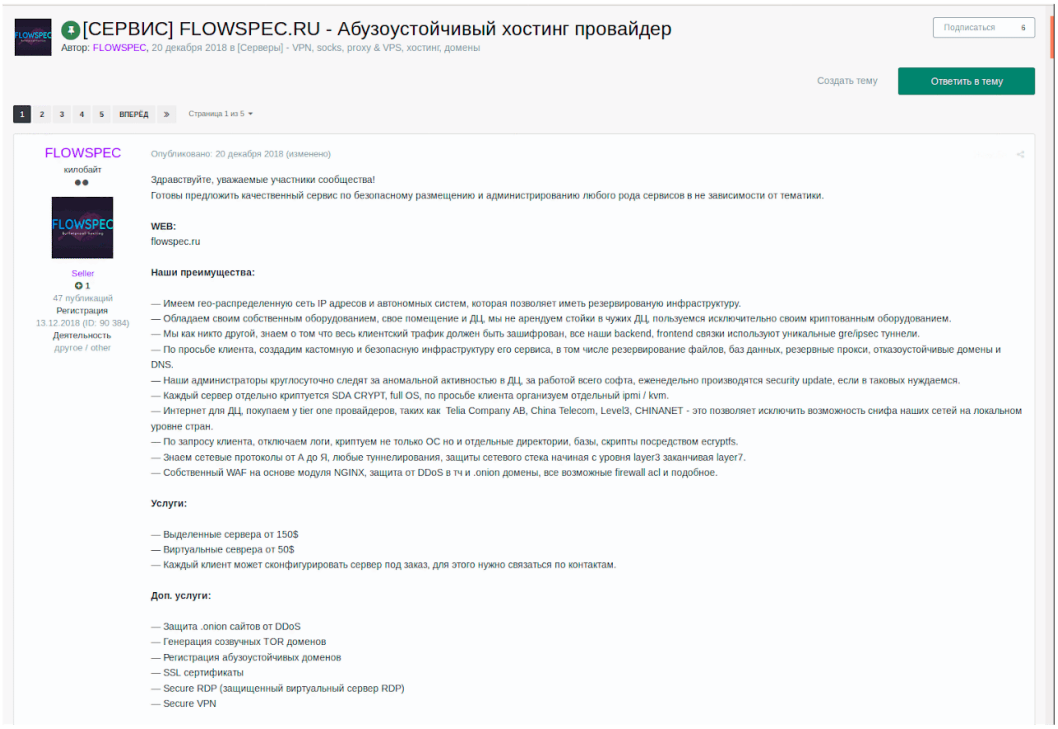
The information gleaned from the RIPE DB and from RIPEStat is somewhat more reliable than domain WHOIS as it can't all simply contain dummy data and some of it is related to BGP, which needs to be legitimate if you're going to play on the internet. To summarize some of the info we've pulled together:

- Both IPs are part of 176.121.14.0/24, which is a relatively small netblock of 256 IP addresses
- The prefix falls under ASN 210138, which was created on Oct 2, 2019
- The AS first announced 176.121.14.0/24 on Oct 12, 2019
- The prefix and ASN are associated with a company called Flowspec LTD

Next, we consider the question of whether or not this particular organization is catering its services to cybercriminals directly in the underground marketplace. A quick look across a number of forums will show that Flowspec is operating in plain sight and clearly offering bulletproof hosting services. It's not always this easy to answer this question, however.

```
person:          Mr. James Hayes
address:         Belize City, Belize
phone:           +501 721 0024
e-mail:          abuse@flowspec.online
nic-hdl:         NS7363-RIPE
mnt-by:          FLOWSPEC-MNT
created:         2018-07-29T18:15:42Z
last-modified:   2019-03-17T02:14:30Z
source:          RIPE
```

RIPE Database Software Version 1.97.2



We've taken an abbreviated look at Flowspec's setup, but what we can conclude is that TA505 are likely active in the underground marketplace and using the BPH services of Flowspec. It's a safe bet to also conclude that nothing good is coming out of Flowspec's /24 and it's more or less set aside for nefarious activity. TA505, a somewhat sophisticated adversary, are just one of a number of clients so to block that /24 will also help defend against any other badness originating from Flowspec.

So what can we do about it?

Course of action (COA) analysis must take into account your organization's capabilities, but below are a number of simple COAs that might make this sort of research and analysis actionable for your organization.

1. Block/alert on all 256 IPs associated with 176.121.14.0/24. The prefix is owned and operated by a known BPH service. One of the service's clients is TA505. Better yet, blacklist the ASN and any prefixes associated with it.
2. Monitor the 176.121.14.0/24 for BGP announcements that would suggest it is being removed from Flowspec or moved to another entity. This could indicate the prefix is no longer used as part of the BPH service or has been transferred to a new entity under the service's control.
3. Monitor BGP announcements for Flowspec's ASN to identify new prefixes being added so you can immediately block/alert on them.
4. TA505 Webinar – 23 July 2020

Want to learn more about TA505?

Join us on July 23rd, 2020 for our TA505 Deep Dive webinar that will cover the group's history including TTPs.

Register at:
https://us02web.zoom.us/webinar/register/WN_Z_YvCOXHRweL6vW3EoqO2Q